SECURITY INTELLIGENCE
REVIEW COMMITTEE

BUILDING FOR TOMORROW:
THE FUTURE OF SECURITY INTELLIGENCE ACCOUNTABILITY IN CANADA

ANNUAL REPORT
2017–2018

Canada

Security Intelligence Review Committee
P.O. Box 2430, Station D Ottawa ON K1P 5W5

Visit us online at www.sirc-csars.gc.ca

© Public Services and Procurement Canada 2018

Catalogue No. PS105E-PDF
ISSN 1921-0566

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

May 31, 2018

The Honourable Ralph Goodale
Minister of Public Safety and Emergency Preparedness
House of Commons
Ottawa, Ontario K1A 0A6

Dear Minister Goodale:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for fiscal year 2017–2018, as required by section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

Pierre Blais, P.C.
Chair
Appointed May 1, 2015

L. Yves Fortier, P.C., C.C., O.O., Q.C.
Appointed August 8, 2013

Gene McLean, P.C.
Appointed March 7, 2014

Ian Holloway, P.C., C.D., Q.C.
Appointed January 30, 2015

Marie-Lucie Morin, P.C., C.M.
Appointed May 1, 2015

ABOUT SIRC

The Security Intelligence Review Committee (SIRC or "the Committee") is an independent, external review body that reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS).

SIRC is responsible for ensuring that the extraordinary powers given to CSIS by Parliament to intrude on the privacy of individuals are executed in a manner that respects the rule of law and the rights and freedoms of Canadians.

SIRC uses its authority to examine all information under CSIS's control, no matter how classified or sensitive, with the exception of Cabinet confidences, to perform SIRC's three core functions: carrying out in-depth reviews of CSIS's activities, conducting investigations into complaints, and certifying the CSIS Director's annual report to the Minister of Public Safety and Emergency Preparedness.

SIRC's findings are summarized and edited to protect national security and personal privacy, then published in annual reports tabled in Parliament. Visit SIRC online at www.sirc-csars.gc.ca for more information.

ABOUT THE COMMITTEE

The Committee is composed of the Honourable L. Yves Fortier, the Honourable Ian Holloway, the Honourable Gene McLean, and the Honourable Marie-Lucie Morin, and is chaired by the Honourable Pierre Blais.

Located in Ottawa, SIRC is supported by an Executive Director and an authorized staff complement of 31 that includes a Deputy Executive Director and General Counsel, a Director of Research, and a Senior Corporate Services Manager, as well as other professional and administrative staff.

The Committee approves direction on research and other activities that have been identified as a priority for the year. Day-to-day operations are managed and delegated to the Executive Director with direction, when necessary, from the Chair, who serves as Chief Executive Officer.

An important function of Committee members is to preside over the investigation of complaints from the public through a quasi-judicial process. Committee members, along with senior staff, also participate in regular discussions with the executive and staff of CSIS, as well as with other members of the national security community as part of their ongoing work. These exchanges are supplemented by discussions with academics, security and intelligence experts, and other relevant organizations as needed. Such activities enrich SIRC's knowledge about issues and debates affecting Canada's national security landscape.

For the purpose of review, Committee members and SIRC staff visit CSIS regional offices to understand and assess the day-to-day work of investigators in the field. These visits give SIRC an opportunity to be briefed by regional CSIS staff on local issues, challenges, and priorities, while allowing SIRC to communicate its focus and concerns.

TABLE OF CONTENTS

MESSAGE FROM THE COMMITTEE 4

MESSAGE FROM THE ACTING EXECUTIVE DIRECTOR 8

1
CERTIFICATION OF THE CSIS DIRECTOR'S ANNUAL REPORT TO THE MINISTER 10

2
REVIEWS 13

The Review Process at SIRC 13

Case Studies Regarding CSIS Information Sharing with Foreign Entities 15

CSIS's Approach to Mental Health in CSIS Investigations 18

CSIS's Right-Wing Extremism Investigation 19

CSIS's Use of the Internet in Support of Operations 20

Foreign Stations 21

CSIS's Operations in Dangerous Environments 22

CSIS's Threat Reduction Measures 23

3
SECTION 54 REPORT: CSIS'S RESPONSE TO THE FEDERAL COURT DECISION OF OCTOBER 2016 25

4
COMPLAINT INVESTIGATIONS 34

Allegations of Religious Profiling and Conspiracy: Complaint Pursuant to Section 41 of the *CSIS Act* 35

Allegations of Delay and Racial Prejudice in a visa application: Complaint Pursuant to Section 41 of the *CSIS Act* 37

Allegations that CSIS Collected Information about Canadian Citizens and Groups Engaged in Peaceful and Lawful Activities: Complaint Pursuant to Section 41 of the *CSIS Act* 38

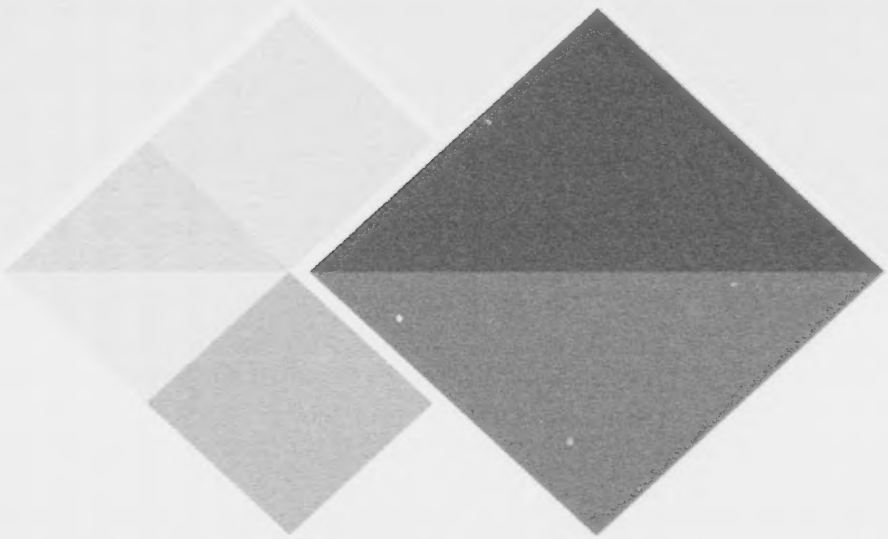
Denial of Security Clearance: Complaint Pursuant to Section 42 of the *CSIS Act* 38

5
RECOMMENDATIONS 40

6
CORPORATE OPERATIONS 47

7
ANNEX 49

MESSAGE FROM THE COMMITTEE



At the time of writing, Bill C-59 remains a draft and with it the government's proposal to create the National Security and Intelligence Review Agency or NSIRA, which would be responsible for reviewing intelligence and national security activities across government. If NSIRA is formed as currently outlined in Bill C-59, the dedicated national security review of the type that SIRC has been doing for more than 30 years for CSIS will be established for all departments and agencies with responsibility for national security and intelligence.

The government has signaled a new direction for accountability through a system that combines NSIRA with an Intelligence Commissioner, and the newly created National Security and Intelligence Committee of Parliamentarians. With that in mind, one of the Committee's immediate priorities is its engagement with this committee of parliamentarians.

Despite the prospect of change in the near future, over the past year, the Committee has remained focused on its first priority: to discharge its mandate under its enabling legislation, the *Canadian Security Intelligence Service Act* (*CSIS Act*), to provide assurance to Parliament and Canadians with respect to the lawfulness of CSIS's activities and to investigate complaints. The Committee is pleased to report that SIRC's reviews touched on the full range of CSIS activities.

In addition to examining large samples of CSIS's core activities to support the certification process, SIRC conducted reviews that delve deeply into specific operational activities, the results of which are summarized in this report. In addition to findings specific to each review, SIRC noted a broader capacity gap with respect to the development and renewal of operational policies that was evident across several reviews from this year, as well as some reviews from previous years. This gap has resulted in situations in which operational policies are out of step with CSIS's evolving operational activities and current jurisprudence. These gaps could put CSIS at greater risk of non-compliance with the law, among other risks. As always, SIRC will continue to be attentive to issues such as these in the future.

Work continues in other ways as well. The Committee is pleased to report that SIRC actively engaged a range of government and non-governmental partners throughout the reporting cycle, including academics and civil society representatives. Of particular note, the Committee recently met with its counterpart organizations from the "Five Eyes" countries. SIRC led a discussion on enhancing working-level contacts and cooperation to address the gap that others have noted, which is that review bodies need to match intelligence cooperation with better cooperation between review bodies.

While continuing to discharge its current mandate to review CSIS's activities, SIRC has in mind the possibility of change in the near future. The proposed legislation provides that SIRC's current staff will carry over to the new agency, NSIRA, and the Committee members will continue in their functions until the end of their mandate. Anticipating this change from SIRC to NSIRA, it is appropriate now to reflect on SIRC's history, as we look to the future.

SIRC was created to provide assurance to Parliament and, by extension, Canadians that CSIS investigates and reports on threats to national security in a manner that respects the law and the rights of Canadians. Over its more than 30-year history, SIRC has discharged its mandate faithfully and it has had an important impact on accountability in Canada's national security framework.

BILL C-59

In the House of Commons on November 20, 2017, the Minister of Public Safety and Emergency Preparedness, the Honourable Ralph Goodale, made the following statement:

"One of the major advances in this legislation is the creation of the national security and intelligence review agency. This new body, which has been dubbed by some as a 'super SIRC,' will be mandated to review any activity carried out by any government department that relates to national security and intelligence, as well as any matters referred to it by the government."

SIRC's findings and recommendations have extended to the core of CSIS activities and have touched on some of the most sensitive operations. They have also prompted change at all levels, from changes to CSIS's operational policy, to renewed direction from the Minister, to changes to the *CSIS Act*. It has always been SIRC's view that it is working to make CSIS a better organization, one that is able to respond effectively to a changing threat environment, and in a manner that respects the rights of Canadians. CSIS itself has acknowledged the impact that SIRC has had over the years. Most recently, former Director Coulombe stated that "SIRC's ongoing reviews contribute to a culture of continual learning and improvement. We welcome the review process and believe it has helped make us a better organization."

The earliest work of SIRC focused on the building blocks of CSIS as it was created from the Royal Canadian Mounted Police (RCMP) Security Service. Much of this period was occupied with establishing the parameters around its engagement with CSIS. Maurice Archdeacon, SIRC's first Executive Director (1985–1999), recalled that the earliest meetings between CSIS and SIRC were far from cooperative or constructive. "CSIS pushed back constantly against our efforts... and we regularly found ourselves in long waits for responses to our requests." After more than three decades, the relationship between SIRC and CSIS has matured. Although there continue to be occasional areas of disagreement, there is no question that CSIS accepts SIRC's mandate and has organized itself to support SIRC's work as an independent review body. This experience will serve NSIRA well as it establishes these same terms of engagement with the new departments and agencies under its purview. Indeed, SIRC's productive relationship with CSIS will set the standard for NSIRA's interactions with these new departments and agencies.

With the exception of the added responsibility for certifying the Director's report to the Minister in 2012, SIRC's mandate has not changed since its inception in the 1980s. How that mandate has translated into specific areas of review, however, has changed. SIRC has followed CSIS as its priorities have shifted since the end of the Cold War when counter-intelligence was the dominant threat, and again after 9/11 with the rise of extremism.

What have these changes meant for SIRC? As CSIS's priorities change and it is confronted with new challenges, and as new sets of interests and rights are brought into the frame, it is SIRC's responsibility to understand these trends and react accordingly. Most recently, a priority for CSIS, and the government as a whole, has been the foreign fighter threat. Correspondingly, understanding the unique challenges of this investigation, and making recommendations whenever possible, has become a continuing priority for SIRC. This is evidenced by the recent reviews on aspects of CSIS's foreign fighter investigation. SIRC's experience suggests that maintaining relevance depends on being attentive to, and nimble in the face of, CSIS's evolving priorities and tradecraft.

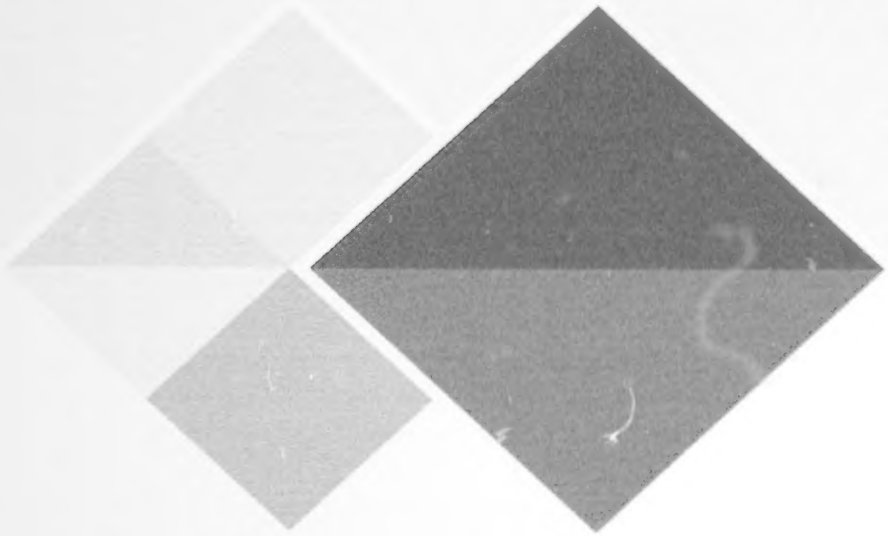
As the guardian of the *CSIS Act* since it was drafted in the 1980s, SIRC has also been attentive to signs of strain between the powers provided to CSIS in the *Act* and the evolution of intelligence work. SIRC has made the observation several times in its history that the *CSIS Act* is showing its age. Mindful of its mandate with respect to lawfulness, SIRC has always sought to position itself where those tensions are most acute. Such was the case with SIRC's work with respect to metadata and bulk data collection.

Throughout its history, SIRC has sought to find the balance between its responsibility to defend the rights of citizens to privacy and civil liberties, and the right of the state to defend against threats. SIRC is hopeful that the consultations and parliamentary deliberations now taking place in the context of Bill C-59 will help NSIRA as it prepares to meet the public's expectations of it.

Looking at the experience of other review bodies internationally, it is clear that changes to Canada's system of accountability are happening at a time when there has been a shift in thinking on accountability for intelligence agencies, translating into public expectations of greater transparency. To that end, Bill C-59 provides for NSIRA to issue special reports when it decides that it is in the public interest to do so. It is the Committee's hope that Canada, and NSIRA, will in this way continue to respond equally to the shifting needs of intelligence and security agencies, as to shifts in public expectations.

From left to right: Ms. Marie-Lucie Morin, Mr. Pierre Blais, Mr. Gene McLean, Mr. Yves Fortier, Dr. Ian Holloway. © 2016 BalfourPhoto

MESSAGE FROM THE ACTING EXECUTIVE DIRECTOR



As always, SIRC is pleased to present this annual report and, in it, to highlight some of the more substantial outcomes during the reporting year.

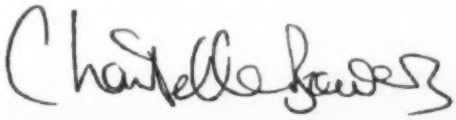
On the review side, we are continuing to refine our planning tools based on the principles outlined in our newly implemented risk-based planning matrix. This will ensure that the reviews for the next fiscal year provide as much coverage of high-risk issues as possible. SIRC is also moving to a three-year research plan to ensure that all CSIS programs and activities are reviewed on a more regular and cyclical basis.

In this past year, we completed the largest-ever number of reviews. Included among them were two special reports prepared following the Minister's request that SIRC review CSIS's response to the October 2016 Federal Court decision on the illegal retention of non-threat-related metadata acquired under warrant. A number of reviews are also noteworthy for their scope and depth, featuring an extensive number of interviews in the context of the review of CSIS's activities in dangerous environments and, to support the certification process, a large sample of CSIS's core activities: targeting, human sources, and warrants. Consistent with our commitment to review more foreign activity, we also reviewed three foreign posts during this research cycle.

Similar strides were made in the investigation of complaints, with SIRC's investigations process further refined and streamlined based on best practices. This is a central focus of our strategy to improve access to SIRC's investigations process, as well as its timeliness. Accordingly, SIRC will continue to assess its Rules of Procedures to ensure that Canadians receive a timely answer to their complaints against CSIS, while respecting the principles of fundamental justice.

I will also take the opportunity to note that, alongside the outreach activities of the Committee, SIRC staff appeared at a number of conferences and events during the reporting period. The importance of our outreach activities cannot be overstated, as they ensure that we understand the range of views on matters connected to its mandate.

At the same time, we are looking to the future of review in light of the proposed new agency, NSIRA, included in Bill C-59. The proposed legislation makes clear that SIRC and its experience as an expert review body for more than 30 years will be central to changes in the national security landscape. With this in mind, SIRC continues to use its capacity funding to add to our staff of legal counsel and reviewers to provide as much capacity to NSIRA as possible.



Chantelle Bowers
Acting Executive Director

1 CERTIFICATION OF THE CSIS DIRECTOR'S ANNUAL REPORT TO THE MINISTER

Pursuant to subsection 38(2) of the CSIS Act, *SIRC is required to submit to the Minister of Public Safety and Emergency Preparedness a certificate stating:*

- the extent to which it is satisfied with the CSIS Director's annual report to the Minister;
- whether the operational activities described in the Director's report contravened the *CSIS Act* or ministerial directions; and
- whether the activities described in the report involved any unreasonable or unnecessary use of CSIS's powers.

This certificate, therefore, provides an important high-level assessment of the legality, reasonableness, and necessity of CSIS's operational activities.

To fulfill its responsibility for the certification process, SIRC relies on a carefully designed and rigorous research methodology. To that end, SIRC conducts an extensive review of CSIS information holdings and requests briefings with CSIS officials to ensure that the information in the Director's report is placed in its proper context. SIRC grounds its assessment in reviews of several specific operations and activities referred to in the Director's report.

SIRC's ongoing baseline and thematic review work, which yields important findings and recommendations, directly supports the certification process. In addition, SIRC conducts three core reviews of human sources, targeting, and warrant execution. These reviews include examining samples of each core function based on the investigations covered in the Director's annual report. SIRC assesses all its reviews against CSIS's compliance with the *CSIS Act* and ministerial direction in order to determine whether SIRC considers any use by CSIS of its powers to be unreasonable or unnecessary.

SATISFACTION WITH THE DIRECTOR'S ANNUAL REPORT

The Committee's satisfaction with the Director's report is based on SIRC's assessment of the extent to which the report provides the Minister with information to assist in exercising ministerial responsibility for CSIS. First, SIRC examined whether the report satisfied the ministerial requirements for reporting. Second, SIRC assessed whether the statements made in the report were factually accurate, well supported, and placed in the proper context. Third, SIRC ensured that the information was representative of CSIS activities during the period under review. SIRC reviewed CSIS documents and considered its own review findings during the time period to ensure that no significant issues or operations were omitted. SIRC also assessed all relevant briefings that CSIS provided to the Minister with the same criteria used to assess statements in the report.

The Committee was satisfied with the Director's report. SIRC found that CSIS fulfilled ministerial reporting requirements, information was placed in its proper context and the content of the report was an accurate representation of CSIS's activities.

COMPLIANCE WITH THE *CSIS ACT* AND MINISTERIAL DIRECTIONS AND EXERCISE OF CSIS'S POWER

The *CSIS Act* also requires the Committee to state whether, in its opinion, the operational activities described in the Director's report contravened the *CSIS Act* or ministerial direction, including direction on intelligence priorities, and whether the activities involved any unreasonable or unnecessary use of CSIS's powers. SIRC conducted core reviews on sources, targeting, and CSIS's execution of Internet warrants. These reviews were designed to assess CSIS's compliance and identify any unreasonable use of its powers. SIRC reviewed documents in CSIS's holdings used to prepare the report and the Minister's case-by-case briefings. The results of SIRC's yearly reviews were also considered.

SIRC is concerned with cases of non-compliance related to information sharing. SIRC concluded in its review of information sharing summarized in this report that there was one case in which there were instances when CSIS did not adequately assess and mitigate the potential risk of sharing information as required by the 2011 *Ministerial Direction to the Canadian Security Intelligence Service: Information Sharing with Foreign Entities*. SIRC's core review of targeting also found that there were three instances of non-compliance with internal policy concerning information sharing having to do with terminating investigations. As SIRC has noted in the past, it will continue to make information sharing an integral part of its annual reviews and certification process.

This year, SIRC also examined a sample of the non-compliance incidents identified by CSIS's internal compliance regime, which were reflected in the Director's report. SIRC assessed the majority of the non-compliance incidents identified by both SIRC and CSIS and concluded they were due to human error rather than a failure of policy or willful disregard on the part of a CSIS employee. In addition, there were instances of non-compliance due to the errors or actions of the communications service providers.

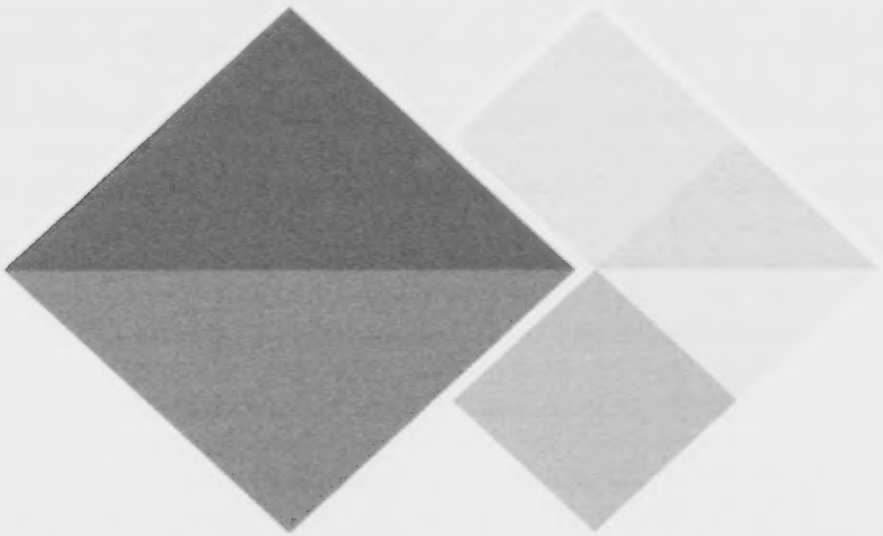
However, SIRC noted one instance of non-compliance with respect to a warranted power that was executed without reasonable grounds to believe that it would result in the collection of information on the subject of the investigation. SIRC determined this was the result of numerous errors and oversights on the part of CSIS. The error was identified by CSIS and subsequently reported and investigated in a manner consistent with CSIS's internal compliance process. SIRC is satisfied that CSIS's internal compliance process functioned as it should. Just after the period under review for this certificate, the Director determined that a report as per section 20 (2) of the *CSIS Act* should be completed. The Federal Court was also informed of the error.

The Committee is of the opinion that, with the exception of the retention of specific bulk datasets reported to the Minister in SIRC's section 54 review of CSIS's response to the Federal Court decision, and notwithstanding the examples highlighted above, the activities described in the Director's report and those assessed as part of SIRC's review activities complied with the *CSIS Act* and ministerial direction, and did not constitute an unreasonable or unnecessary exercise of CSIS's powers.

THREAT REDUCTION MEASURES

CSIS is required to report on its threat reduction measures in the Director's annual report. SIRC is also obligated to review threat reduction measures annually, which it does through an annual stand-alone review. For this reporting cycle, SIRC found that the threat reduction measures that SIRC examined complied with the *CSIS Act*, ministerial direction, and operational policies. SIRC can further report that no warrants were issued under section 21.1 of the *CSIS Act*, nor were any applications for warrants refused.

2 REVIEWS



THE REVIEW PROCESS AT SIRC

SIRC's reviews are designed to provide Parliament and the Canadian public with the assurance that, in the performance of its duties and functions, CSIS has acted appropriately, effectively, and in accordance with the rule of law. SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and activities, which include: counter-terrorism, counter-intelligence, counter-proliferation and security screening. The reviews also examine CSIS's arrangements to cooperate with foreign and domestic organizations, as well as the advice CSIS provides to the Canadian government.

At the beginning of each fiscal year, SIRC researchers develop a research plan that is presented to the Committee for approval. This plan is meant to address a broad range of subjects on a timely and topical basis, taking into consideration such matters as:

- activities by CSIS that could have an impact on individual rights and freedoms;
- new investigative activities, directions, and initiatives announced by or affecting CSIS;
- intelligence priorities identified by the Government of Canada;

- events or developments with the potential to represent threats to the security of Canada;
- issues identified in the course of SIRC's complaints functions; and
- the CSIS Director's annual report submitted to the Minister of Public Safety and Emergency Preparedness.

THE YEAR AHEAD

In 2018–2019, SIRC will be looking at the full range of CSIS activities, anchored in its reviews of CSIS's core activities involving targeting, warrants and special operations, and human sources. SIRC will continue to examine CSIS's activities abroad, with planned reviews of two foreign stations. Throughout, SIRC will balance the need for comprehensive coverage of CSIS's investigative activities, with its ongoing focus on areas of highest risk to SIRC's central concern, which is the lawfulness of CSIS's activities.

As part of this process, SIRC's researchers consult multiple information sources to examine specific aspects of CSIS's work, such as: operational reporting, individual and group targeting files, human source files, intelligence assessments, and warrant documents. The examination of these documents generates follow-up exchanges with CSIS in the form of meetings and briefings that allow SIRC researchers to seek clarification and ensure a complete understanding of the issues at hand.

Each completed review includes findings and, where appropriate, recommendations. These reviews are forwarded to the Director of CSIS and the Minister of Public Safety and Emergency Preparedness and — after being edited for national security and privacy considerations — are made available in the annual report tabled in Parliament.

SIRC'S METHODOLOGY

SIRC employs a common framework, or set of core criteria, to guide and support its examination of CSIS's activities. These criteria include legal thresholds contained in the *CSIS Act* (e.g., reasonableness, proportionality, and strict necessity), and whether the activity complies with ministerial direction, adheres to principles of good governance, and follows CSIS's policy framework and procedures. SIRC assesses CSIS's activities as effectively as possible through a carefully selected combination of review methods. Each review produced by SIRC falls in one of the following categories.

Thematic reviews: these horizontal reviews are designed to give a broad view of a particular issue or theme that cuts across CSIS programs or investigations. These reviews often provide SIRC's most substantive findings and recommendations.

Investigation/program reviews: these reviews examine a particular CSIS investigation or area. They are valuable in that they allow SIRC to maintain knowledge of priority investigations on a regular basis.

Baseline reviews: these reviews are designed to gain insight into a CSIS activity that had not previously been the subject of in-depth, focused review. They offer insight into a new activity, investigation, or program.

Core reviews: these reviews offer insight into CSIS's main activities — that is, targeting, warrants, and the use of human sources — through a larger sample analysis. These reviews provide an opportunity for SIRC to drill down more deeply into a specific type of activity.

SIRC relies on risk-based planning to provide a comprehensive and meaningful review of CSIS's activities. Due to SIRC's small size, it is impractical for it to examine all of CSIS's duties and functions annually. Risk-based planning allows for and ensures that all CSIS activities are reviewed regularly and systematically.

RECOMMENDATIONS

SIRC's reviews include findings and, where appropriate, recommendations. Guidelines regarding recommendations have been developed to ensure they are practical, constructive, and focused on tangible actions and results.

To provide greater transparency and insight into the impact of SIRC's work on security intelligence, SIRC actively solicits CSIS's formal responses to its recommendations and includes them in its annual report summaries.

These responses are expected to clearly and unambiguously indicate whether CSIS agrees or disagrees with the recommendation, what actions CSIS intends to take in response, and when it intends to take such action.

Although SIRC's recommendations are non-binding, CSIS has implemented a large percentage of them, as noted in SIRC's annual departmental performance reports (now called departmental results reports), and has publicly acknowledged that it has become a better organization because of SIRC.

CASE STUDIES REGARDING CSIS INFORMATION SHARING WITH FOREIGN ENTITIES

SIRC last reviewed CSIS information sharing with foreign entities in 2015 and found problems with respect to the consistency and documentation of decisions made by CSIS operational managers in cases where the potential for mistreatment existed.

This review followed up on these findings by examining four cases concerning CSIS information sharing with foreign entities between 2015 and 2017 where a substantial risk of mistreatment existed; the four cases were divided between two countries known to have problematic human rights records.

SIRC approached this review through the lens of the 2011 *Ministerial Direction to the Canadian Security Intelligence Service: Information Sharing with Foreign Entities* (replaced in 2017 — see "Section 17 of the *CSIS Act*" on page 16), which requires CSIS to "assess and mitigate potential risks of sharing information in ways that are consistent with its unique role and responsibilities." At an operational level, this direction requires that CSIS determine whether there is a substantial risk of mistreatment in a given instance of information sharing. If there is, and it is unclear whether the risk can be mitigated, the decision must be referred to the Director of CSIS. This is done through the Information Sharing Evaluation Committee (ISEC), which includes senior CSIS officials and representatives from other government departments.

SECTION 17 OF THE *CSIS ACT*

Section 17 of the CSIS Act *authorizes CSIS, with the approval of the Minister, to enter into formal arrangements with domestic and foreign partners for the purpose of performing its duties and functions. Among other things, these arrangements can allow CSIS to exchange information and/or engage in joint operations with foreign partners, depending on the terms of the arrangement.*

Information sharing with foreign partners is limited by ministerial direction. In September 2017, the 2011 Ministerial Direction to the Canadian Security Intelligence Service: Information Sharing with Foreign Entities *was replaced by the new* Ministerial Direction to the Canadian Security Intelligence Service: Avoiding Complicity in Mistreatment by Foreign Entities.

Risk of mistreatment is generally mitigated using caveats and assurances. Caveats are limitations on use attached to intelligence products that are shared with partners. For example, one caveat stipulates that the information being shared is for intelligence purposes only and should not be used in a prosecution or shared with other agencies without the consent of the originator; this is known as the Third Party Rule. Assurances are verbal and/or provided through written agreements between foreign agencies. Generally, the receiving country provides assurances that the originator's caveats and expectations pertaining to human rights will be respected.

In each instance, SIRC evaluated whether the risks associated with sharing or requesting information were appropriately documented. Where mitigation measures were used, SIRC expected that the risk of these measures not being adhered to would have been appropriately assessed and documented. Where it was unclear whether the risk could be mitigated, SIRC expected that these cases would have been referred to ISEC. Finally, SIRC examined the fate of the individuals involved for evidence that CSIS information sharing had directly contributed to human rights abuses.

The reliability of assurances to mitigate the risk of torture or mistreatment depends on a number of contextual factors. SIRC considered the following to be the most important: (1) the human rights record of the state and agency in question; (2) the length and strength of bilateral relations between the two states; and (3) the other state's record in abiding by the assurances in the past.

Over the course of the review, SIRC found no evidence that CSIS used information obtained by torture and other cruel, inhuman, or degrading treatment, nor directly contributed to human rights abuses when it shared information in these cases.

However, SIRC found in two of the cases reviewed that the risks of sharing or soliciting information, as well as the risk that caveats and assurances would not be respected, were not appropriately assessed or documented by operational managers. The corporate documentation available to operational managers generally lacked the information necessary to make an assessment regarding mitigation.

Moreover, SIRC found that CSIS shared and requested information with respect to a Canadian detained by a foreign state without the approval of ISEC, despite evidence of an elevated risk that the caveats and assurances would not be respected. In this case, CSIS continued to rely on assurances it had received from this country five years prior, despite having committed to the Minister of Public Safety and Emergency Preparedness to seek updated assurances due to credible allegations of torture.

Finally, at the strategic level, SIRC found that CSIS did not have any documented criteria or thresholds that would trigger a re-evaluation of the relationships with these countries in response to intelligence suggesting that assurances were not being adhered to.

SIRC will continue to monitor CSIS's activities with respect to information sharing with foreign entities as its policy and processes in this area evolve, in particular, with respect to CSIS's application of the most recent information sharing ministerial direction released in September 2017.

SIRC recommended that:

- CSIS prioritize the development of guidelines on assessing and documenting the risk of mistreatment as well as the risks of assurances and caveats not being respected — such assessments should take into account the most recent and relevant information, including operational reporting.

CSIS response:

CSIS agreed with this recommendation.

In addition to robust existing guidelines on assessing and documenting the risk of mistreatment, CSIS is adopting a new model for restricting exchanges with foreign agencies.

This new approach has three clear objectives: (a) ensuring that CSIS' engagement with a foreign partner does not pose a substantial risk of mistreatment; (b) only allow sharing of information which is not deemed to present a potential risk of mistreatment; and (c) ensuring full compliance with the Ministerial Directive.

SIRC further recommended that:

- when there is a substantial risk of mistreatment in sharing or requesting information that needs to be mitigated, the decision to share should be referred to the Director through the Information Sharing Evaluation Committee rather than an operational manager.

CSIS response:

CSIS agreed with this recommendation.

Ministerial Direction is enshrined within CSIS directives on information sharing when there is a risk of mistreatment. Moreover, CSIS has adopted a new model for restricting exchanges with foreign agencies in which proposed exchanges of information deemed to be high risk must automatically be referred to the Information Sharing Evaluation Committee and others will be prohibited outright.

CSIS'S APPROACH TO MENTAL HEALTH IN CSIS INVESTIGATIONS

SIRC reviewed CSIS's approach to mental health issues. SIRC had previously observed that mental health issues are more and more frequently becoming a factor in CSIS investigations.

SIRC examined a sample of CSIS's files with a mental health component between January 1, 2014 and June 30, 2017, and is satisfied that CSIS's approach to mental health issues was appropriate and conformed to ministerial direction.

SIRC noted the high value of specialized mental health expertise and its impact at the operational level. CSIS relies on mental health experts for a variety of functions. The resulting demand for their assistance surpasses their capacity, given finite resources. This creates a backlog, delays, and a constant triaging of priorities. Furthermore, SIRC noted that not all cases are referred to CSIS experts because CSIS officers know they are overburdened and will not be able to respond in a timely manner.

SIRC found that without any proper protocol in place on when to consult these experts, CSIS personnel make subjective judgments on when to request their professional assistance. In addition, SIRC was informed that files are referred, or requests made, for advice at varying points — some too early to provide adequate analysis and some too late to be of any assistance to an investigation. SIRC found that CSIS's experts are not being used to their potential and that this ambiguity could hinder investigations.

SIRC recommended that:

- CSIS increase the resources available to keep up with the demands for services that assist CSIS to manage mental health issues that arise in CSIS investigations.

CSIS response:

CSIS partially agreed with this recommendation.

CSIS has been working to address vacancies and has also explored other strategies to increase these capabilities. CSIS will consider these requirements in any future resource allocation exercises, while also taking into account competing requirements in other priority areas.

SIRC further recommended that:

- CSIS create a specific reference tool to be relied upon to identify general mental health issues.

CSIS response:

CSIS agreed with this recommendation.

CSIS sees value in the creation of this tool as it will assist CSIS officers in identifying general mental health issues in a proactive fashion.

CSIS AND LAWFUL DISSENT

CSIS's mandate under section 12, which is to investigate "threats to the security of Canada," is constrained by the definition of the term laid out in section 2 of the Act. In addition to prescribing the four types of activities that qualify as "threats to the security of Canada," section 2 also specifically excludes "lawful advocacy, protest, or dissent."

CSIS'S RIGHT-WING EXTREMISM INVESTIGATION

The killing in early 2017 of six Muslims at a mosque in Québec raised questions regarding CSIS's investigation into extremist behaviour that is not associated with Islamist extremism. This year, SIRC examined CSIS's activities since 2012 with respect to right-wing extremism investigations as well as the impact, if any, of the January 2017 killings on CSIS's investigations. One objective of this review was to determine how CSIS has investigated right-wing extremism since SIRC last examined this as part of its 2012 review, "CSIS Activities Related to Domestic Investigations and Emerging Issues."

CSIS characterizes right-wing extremism in Canada as a movement that includes a complex range of groups and individuals espousing a broad range of positions and grievances, including white supremacy, white nationalism and white religion; anti-Semitism; homophobia; nativism and anti-immigration; anti-government and anti-law enforcement; and racism.

As a result of a CSIS internal review, which found that the majority of right-wing extremism activities consisted of, or were "near to," lawful protest, advocacy, and dissent (see highlighted text below), CSIS determined that the current threat environment no longer met the threshold of a CSIS investigation. In addition, CSIS also determined that the public order threat (versus the national security threat) was being appropriately addressed by law enforcement and it questioned the value added of its efforts. CSIS ended its investigation of right-wing extremism in March 2016.

As a result of the attack on the Grande Mosquée de Québec in January 2017, CSIS reopened its investigation of domestic extremism. Following the attack, SIRC has seen CSIS engage more extensively and frequently with the Royal Canadian Mounted Police (RCMP) and other law enforcement partners to better understand the threat posed by right-wing extremism that would fall under CSIS's mandate.

Overall, SIRC found that CSIS activities conducted during the period of January 1, 2012 to June 30, 2017 complied with the *CSIS Act* and ministerial direction on intelligence priorities. CSIS activities were also consistent with the authorities and limitations set out in its targeting policy. SIRC found that partnerships with police and law enforcement agencies and other investigative tools at CSIS's disposal played an important part in the investigation. Besides helping to maintain awareness, these tools were valuable in investigating right-wing extremism activities that may present a threat to the security of Canada, including, for example, hate crimes against Muslims.

In CSIS's Québec Region, SIRC found that CSIS's participation in the Structure de gestion policière contre le terrorisme, and the relationships and effective information exchanges with domestic and international law enforcement and intelligence agencies, helped to eliminate gaps in its investigation of right-wing extremism threats.

The review also sought to provide a broad overview of CSIS's approach to investigating right-wing extremism. According to CSIS, violence is usually infrequent, unplanned, and opportunistic, and is carried out by individuals rather than groups. CSIS reported that, since December 2012, CSIS's investigative efforts regarding right-wing extremism were driven mainly by national and international incidents that were associated with right-wing extremism, one recent example being the attack on the Grande Mosquée de Québec.

SIRC takes note of recent events outside of the period under review — for example, in Charlottesville, Virginia; in a number of European cities; and in Halifax, Nova Scotia — that show the potential threat of violent and non-violent right-wing extremism and highlight differences in respective national laws on free speech and hate speech. SIRC will monitor how CSIS's investigation of right-wing extremism responds to any changes in the level of this threat in Canada. SIRC plans to revisit this subject in the medium term.

SIRC recommended that:

- CSIS determine the extent to which other regions' investigation of right-wing extremism could benefit from the experience of CSIS's law enforcement collaborative model in place in the Québec Region.

CSIS response:

CSIS agreed with this recommendation.

Mechanisms are in place across all regions to ensure effective collaboration exists between CSIS and domestic law enforcement bodies.

CSIS'S USE OF THE INTERNET IN SUPPORT OF OPERATIONS

Today's security environment demands effective means to investigate threat-related online activities. SIRC last reviewed this theme as part of its review, "CSIS's Use of the Internet." Since that time, both the legal landscape and CSIS's operational use of the Internet have changed considerably.

SIRC found the manner in which CSIS used the Internet to further its investigations to be a reasonable and necessary exercise of its authorities. CSIS responded appropriately to the legal and technological challenges associated with this type of collection. CSIS officers also understood the legal boundaries related to the collection activities being undertaken and were proactive in requesting legal advice when needed. Nonetheless, the lack of clear jurisprudence regarding certain types of activities necessitates that CSIS exercise caution and, in SIRC's view, could benefit from a comprehensive legal review of CSIS's activities by Justice Canada.

SIRC's review also examined CSIS's efforts to ensure the welfare of individuals engaged in these operations. These individuals frequently view undesirable imagery and other forms of content. In the files reviewed, the individuals were well managed, treated ethically, and offered support for mental health issues, when appropriate. Nonetheless, SIRC acknowledged concerns within CSIS that resource limitations are negatively affecting the length of time it can take to obtain the assistance of mental health experts (see Review of CSIS's Approach to Mental Health in CSIS Investigations). SIRC also noted that resource constraints are impacting the availability of training to CSIS officers that manage and provide support to this type of collection activity.

SIRC recommended that:

- CSIS ask Justice Canada to conduct a comprehensive legal review of CSIS's use of the Internet in support of operations.

CSIS response:

CSIS agreed with this recommendation.

CSIS will request that Justice Canada undertake a legal review of key aspects of the use of internet in support of operations. CSIS will continue to adhere to policies and directives on the administration of this program and will seek out legal advice when and where appropriate.

SIRC further recommended that:

- CSIS ensure that those individuals currently engaged in these operations be given training as soon as possible.

CSIS response:

CSIS agreed with this recommendation.

It is standard CSIS practice to ensure designated employees receive the appropriate training.

FOREIGN STATIONS

Every year, SIRC travels to foreign stations to undertake an in-depth examination of CSIS's work overseas. This year, SIRC conducted two reviews of foreign stations. One review examined two stations located in the same geographic region that share similar collection requirements. The other review focused on a single foreign station located in another geographic region.

In its review of the two stations located in the same region, SIRC found that CSIS activities conducted out of both foreign stations between January 1, 2015 and January 31, 2017 complied with the *CSIS Act* and ministerial direction. SIRC further found that CSIS's activities were consistent with CSIS's priorities and intelligence requirements.

All exchanges with foreign partners involving the two stations in this review fell within the scope of the *CSIS Act* section 17 arrangements that were in place. SIRC did find, however, instances of non-compliance with internal policy that required a particular caveat to be attached to documentation when certain information is shared with CSIS's foreign partners. After reviewing over 1,000 documents, SIRC found that this required caveat was not included in over 35 documents.

SIRC also notes that the value of CSIS's presence was illustrated in both stations after each country experienced terrorist attacks. CSIS's presence provided the Canadian mission with the assurance that any intelligence regarding the incidents — or future attacks — would be quickly forthcoming.

In the second foreign station review, SIRC also found that CSIS's activities conducted between January 1, 2015 and November 1, 2017 complied with the *CSIS Act* and ministerial direction, and were consistent with CSIS's priorities and intelligence requirements. All exchanges with foreign partners fell within the scope of the section 17 arrangements that were in place.

In addition to ensuring compliance with the *CSIS Act*, ministerial direction, and CSIS policies and procedures, another objective of all foreign station reviews is to gain a deeper understanding of the liaison activities at these stations in order to understand CSIS's relationships with its domestic and foreign partners. SIRC found in its two reviews that all three stations have maintained positive relationships with their Canadian partners at missions abroad, all of which appear to appreciate CSIS's presence.

SIRC recommended that:

- CSIS institute a quality assurance mechanism to ensure all required caveats are included prior to sharing information with its partners.

CSIS response:

CSIS agreed with this recommendation.

CSIS is preparing updates to caveat policies and procedures that will further improve quality assurance. Furthermore, CSIS is developing training and technological support related to the use of caveats.

CSIS'S OPERATIONS IN DANGEROUS ENVIRONMENTS

Stemming from a study conducted last year on CSIS's new foreign collection platform, SIRC decided to review CSIS activities within dangerous environments, covering three key operational pillars: CSIS personnel, sources, and targets.

As part of the CSIS personnel portion of this review, SIRC interviewed nearly every employee who travelled to, or worked in, a dangerous environment within the past two years. This was complemented by meetings with CSIS management, written questions to internal stakeholders, a detailed review of relevant policies and procedures, and an examination of documentation related to employee activities.

SIRC found that CSIS's process for designating countries as "dangerous operating environments" (DOEs) does not capture important considerations beyond the provision of firearms to employees, especially for employees conducting activities within countries that ostensibly constitute dangerous environments but that have not received the CSIS designation as a DOE. SIRC also found that a communications gap has developed between CSIS management and employees regarding activities within DOEs and that CSIS has not consistently addressed the increased risk to its employees when they operate overseas in these environments.

CSIS acknowledged being in consultation with its legal services in examining laws and regulations where offences could occur (based on activities of CSIS officers or sources). SIRC first raised this concern in 2014, with a recommendation that CSIS put in place formal internal mechanisms to ensure that none of its human source operations were in contravention of relevant Canadian statutes or regulations. More broadly, proposed legislation (i.e., Bill C-59), if enacted, would directly address some of the ongoing concerns raised in this current review on the possibility of CSIS sources (or employees) being in contravention of Canadian law.

In the review on CSIS targets, SIRC examined reporting on targets that were believed to be physically located within conflict zones. SIRC sought to determine whether information was shared to support lethal action, whether pertinent controls (i.e., caveats and/or assurances) were applied appropriately, and whether the information was assessed, as required by ministerial direction. Overall, SIRC found that CSIS appropriately assessed information as required by ministerial direction and applied the required caveats and assurances to mitigate the risk of sharing.

CSIS's duty-of-care extends to wherever a particular employee is working on behalf of CSIS. To that end, SIRC believes that CSIS requires additional clarity for employees being deployed to dangerous environments to help ensure that expectations are appropriately tempered and that roles, responsibilities, and processes are clear and appropriately constructed for overseas activities.

SIRC recommended that:

CSIS develop a comprehensive strategic framework for operating within dangerous environments. The strategic framework should address, among other considerations, the following:

- creating a more sophisticated rationale for designating dangerous environments, and considering the associated implications of such a designation;
- specifying requirements for employee training pre-deployment;
- updating policies and standard operating procedures;
- clarifying stakeholder roles and responsibilities;
- clarifying expectations for and current feasibility of foreign operational support team(s) who provide a number of crucial services for employees deployed in dangerous environments; and
- developing a communications plan between management and employees specifically geared toward high-risk deployments.

CSIS response:

CSIS agreed with this recommendation and will incorporate and update existing guidelines, policies, and procedures into this framework.

CSIS'S THREAT REDUCTION MEASURES

Since July 2015, CSIS has had the legislative authority to take measures to reduce threats to the security of Canada, within or outside of Canada. Pursuant to the *CSIS Act*, SIRC reviews each year "at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada" (see "CSIS's Threat Reduction Powers" on page 25). This year, SIRC reviewed around a half-dozen cases of threat reduction measures approved and executed between January 1, 2017 and October 31, 2017. One of the cases that was approved during this period, but not executed in 2017, will be reported on in next year's review cycle.

SIRC found that the threat reduction measures examined complied with the *CSIS Act*, ministerial direction, and operational policies. Pursuant to subsection 53(2) of the *CSIS Act*, SIRC reported that there were no warrants issued under section 21.1 of the *CSIS Act*, nor was any application for warrant refused.

CSIS'S THREAT REDUCTION POWERS ARE FOUND IN SECTION 12.1 OF THE *CSIS ACT*, WHICH READS:

Threats to the security of Canada means:

1. *If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.*
2. *The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures, and the reasonable availability of other means to reduce the threat.*
3. *The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the* Canadian Charter of Rights and Freedoms *or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1.*

For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power.

3 SECTION 54 REPORT: CSIS'S RESPONSE TO THE FEDERAL COURT DECISION OF OCTOBER 2016

INTRODUCTION

Following the October 2016 Federal Court decision in X (Re), 2016 FC 1105 regarding the illegal retention of non-threat-related metadata acquired under warrant, the Minister of Public Safety and Emergency Preparedness asked SIRC, under section 54 of the CSIS Act, for a special report on CSIS's response to this decision (see "Section 54 Reports" on page 27). SIRC accepted the request.

SIRC's objective in responding to the Minister's request was to evaluate measures taken by CSIS, following the Federal Court decision, to bring its practices into compliance with the law with respect to the collection and retention of information under section 12 of the *CSIS Act*.

In its decision, the Court concluded that the qualifier "to the extent that it is strictly necessary" in section 12(1) of the *Act* imposes an important limitation on CSIS's mandate: "...information collected by investigation or otherwise, accidentally or as spin-off, cannot be retained if it is found to be unrelated to 'threats to the security of Canada.'" The Court found that CSIS had exceeded its lawful authority under section 12 of the *Act* in retaining in its Operational Data Analysis Centre (ODAC) holdings bulk metadata that had been collected under warrant.

SIRC viewed the decision as having significant implications beyond metadata, including for the assessment of third-party communications (i.e., not involving a target of the warrant) collected incidentally under warrant, and information collected and retained in bulk. In particular, SIRC was concerned with datasets collected in bulk that contain information on individuals, hereafter referred to as bulk datasets. These contain records of generally legitimate activities, some portion of which may pertain to threat-related activities.

Prior to the decision, CSIS discovered some issues with its technical systems, calling into question CSIS's ability to comply with warrant conditions generally. In response, CSIS assembled a project team that identified systemic problems with CSIS's processes for acquiring and handling warranted data. The project team was then tasked with the job of overseeing the response to both these systemic issues and certain aspects of the decision and, ultimately, with providing assurance to the Federal Court with respect to CSIS's ability to comply with warrant terms and conditions.

Overall, SIRC concluded that CSIS responded rapidly and effectively with respect to both the illegal retention of metadata and the problems discovered with its warranted collection systems. CSIS has made good progress in improving its management of the business systems underlying its warranted collection. However, it failed to deal fully with the broader implications of the decision for the retention of non-threat-related information. CSIS's policies with respect to both third-party information collected under warrant and bulk datasets collected without a warrant have yet to be fully aligned with the law as described by the Federal Court decision. In addition, SIRC is concerned with respect to CSIS's capacity to deliver policy development commitments.

SECTION 54 REPORTS

Under section 54(2) of the CSIS Act, "The Review Committee may, on request of the Minister or at any other time, furnish the Minister with a special report concerning any matter that relates to the performance of its duties and functions."

Since 1984, SIRC has provided a number of such special reports. In all but a very few cases, including the one reported on in this year's annual report, these were initiated by SIRC on topics that SIRC believed would be of particular importance for the Minister in exercising his or her responsibility for CSIS. In the case of the section 54 review reported on here, the Minister requested a special report from SIRC to verify whether CSIS's practices have been brought into compliance with the law.

METHODOLOGY

Information Collected Under Warrant

SIRC's evaluation was driven by the following questions:

- Has CSIS taken appropriate action with respect to the disposition of the illegally retained metadata and put in place processes to ensure that, going forward, metadata is retained in accordance with the legal framework and warrant conditions?
- Do CSIS policies and processes with respect to assessment and reporting of warranted data provide sufficient protections to individuals who are not named warranted targets.
- Has CSIS made sufficient changes to governance, business processes, and technical systems to ensure that compliance risks are being appropriately managed?

As the review concerned ongoing work, SIRC received regular briefings from the project team assembled to review warranted collection systems, as well as from other relevant personnel at CSIS headquarters, from April 2017 to February 2018. In addition, SIRC received copies of communications with the Federal Court and had full access to relevant corporate records. SIRC also received briefings from personnel at five out of seven regional offices, including personnel responsible for making decisions with respect to the execution of warrants and retention of data collected.

SIRC's central focus in this part of the review that focused on information collected under warrant was to evaluate CSIS's response to the Federal Court's concerns with respect to the protection of third-party communications. SIRC did not verify the approach through a detailed sample review to ensure compliance partly because the new processes have, in most cases, not been fully implemented. This will be the focus of subsequent reviews. However, where possible, a small number of specific cases were highlighted to illustrate broader issues.

Bulk Datasets

SIRC's review of bulk datasets evaluated the following criteria:

- Did CSIS implement appropriate policies and procedures for the management and assessment of the datasets?
- Was CSIS able to demonstrate significant operational value achieved by the exploitation of the datasets?

SIRC reviewed corporate documentation on the rationale for collection and assessment with respect to the privacy interests engaged and the legal risk for all datasets, the retention of which had been approved by July 2017. SIRC examined the evaluation process for the datasets in the context of the Federal Court decision, as well as the legal advice sought and decisions made based on this advice. To understand fully the use and stewardship of the datasets, SIRC examined the detailed workings of the program, from strategic objectives to the activities and technical systems employed. SIRC also examined the contents of the datasets by directly accessing data repositories.

At the same time, SIRC assessed the operational utility of CSIS's exploitation of bulk datasets. For this, SIRC sought from CSIS a range of statistics relating to the use or utility of datasets. However, CSIS does not track the use of its datasets and was therefore largely unable to provide these statistics. As a result, SIRC approached the question of utility by evaluating case studies illustrating the best outcomes that could be identified, similar to the approach used in the UK publication, *Report of the Bulk Powers Review* by David Anderson, QC.

SIRC reviewed in detail 20 cases in which bulk datasets were exploited. In addition, SIRC discussed the utility of certain specific datasets more broadly with operational desks at headquarters. While the evaluation of the utility of metadata acquired under warrant did not fall within the scope of the review, cases of exploitation of such datasets were examined in order to provide a benchmark for the purposes of comparison. In evaluating the selected cases, SIRC looked at the full investigative context in order to understand the role of data exploitation outputs and the relative contributions of various intelligence sources to the investigations.

SIRC developed a framework for assessment based on whether the resulting intelligence product had a major impact, a significant impact, or simply some impact on the investigation. Operational desks provided their evaluation of the significance of the intelligence to their investigations, and SIRC requested briefings for additional details and insight as necessary. In general, CSIS's assessments with respect to specific cases concurred with SIRC's.

FINDINGS

Information Collected Under Warrant

In response to the Federal Court decision, CSIS rapidly "fenced off" (i.e., removed operational access to) all metadata collected under warrants. Subsequently, CSIS assessed its holdings to determine where the metadata that was found to have been retained unlawfully was stored and how to destroy it while minimizing risks with respect to operations.

SIRC is satisfied with CSIS's plan for the disposition of the metadata. While it took roughly a year to begin deletion of the data, SIRC has been assured that approximately 70 percent of the data has been destroyed. The remainder is expected to be destroyed by October 2018. In addition, CSIS has instituted new processes to ensure that all unreported data (that is, data not used in a report) collected under warrant is deleted in accordance with the new warrant conditions.

SIRC examined the case of a dataset assembled largely from third-party communications collected under warrant that was initially retained in 2008. SIRC assesses that its retention breached the conditions of the applicable warrant. In November 2016, after the Federal Court decision was rendered, the dataset was reapproved for retention without assessment for non-threat-related records. SIRC found that this dataset did not fall within the scope of section 12 of the *CSIS Act* and, therefore, in SIRC's view, was retained unlawfully by CSIS. In response to SIRC's report, CSIS fenced off the dataset, pending the development of a plan for its disposition.

With respect to the broader issues around the retention and reporting of third-party communications, CSIS is still dealing with the implications of the decision. SIRC found that CSIS definitions, guidelines, and training with respect to the assessment and reporting of third-party data are currently insufficient. Although SIRC has been assured that improvements are in development, SIRC is concerned with respect to CSIS's capacity to deliver policy development commitments.

With respect to overall compliance risks with CSIS systems and processes, SIRC found that CSIS has made substantial efforts toward identifying systemic compliance risks and has begun to take action to mitigate risks identified. CSIS is in the process of developing new governance processes and training for warrant invocation, and is working on redesigning its business process architecture.

At the same time, despite action in a number of areas, much work remains to be done toward the goal of managing the risk of non-compliance with warrants. This is acknowledged by CSIS. SIRC is concerned that an elevated level of compliance risk will continue to exist until improvements to policies and warrant processes are complete. SIRC will continue to monitor developments, paying particular attention to CSIS's handling of third-party communications.

Bulk Datasets

In response to SIRC's 2015 "Review of Data Management and Exploitation," CSIS promulgated a new policy and procedure governing the collection and management of datasets in August 2016. This policy defined new categories of datasets that could be collected in bulk despite the presence of a significant portion of non-threat-related records.

SIRC found that CSIS's assessment and management of the bulk datasets with respect to privacy interests and legal risk are not satisfactory. With respect to one particular category of datasets, further documentation related to the assessment of the datasets in question was not available when requested by SIRC. SIRC therefore found that CSIS's process and documentation are not sufficient to permit a determination of whether it is in compliance with the law.

SIRC saw no evidence that CSIS had changed its policies and procedures with respect to the collection of bulk datasets in the wake of the October 2016 Federal Court decision, in spite of the implications of the decision for this practice. In the context of the decision, therefore, SIRC finds that there is a risk that CSIS could exceed its existing legislative authorities in the retention of non-threat-related information on individuals not suspected of constituting a threat to national security.

SIRC did not evaluate the entire inventory of datasets in CSIS's holdings exhaustively. However, SIRC assesses that at least one dataset contains information whose collection carries a sufficient level of risk, both with respect to section 12 of the *Act* and the *Charter*, that continued collection without a warrant is unreasonable.

CSIS does not assess bulk datasets for operational utility and thus had difficulty in demonstrating to SIRC the utility of the datasets. SIRC reviewed with CSIS cases of exploitation of the datasets in order to evaluate their operational value. Those with an exploitable domestic nexus are considered to be more valuable by CSIS.

With one exception, CSIS was not able to provide evidence to demonstrate that exploitation of the datasets had delivered significant value for security intelligence investigations. By contrast, SIRC was able to validate examples of the operational value delivered by target-related metadata collected under warrant.

SIRC examined 17 datasets with an exploitable domestic nexus. SIRC did not see evidence that the nexus to threats is strong enough for these datasets to deliver significant utility in terms of lead generation. This issue was exacerbated by poor data quality. For example, there were a number of cases of mistaken identity due to poor attribution in the dataset used.

The challenges outlined above with respect to CSIS's assessment of datasets should be situated within the context of broader issues concerning the management of ODAC. ODAC encountered significant challenges in achieving its objectives in its early years, and successive reviews of the program made a number of recommendations, including the implementation of a system to measure performance. Overall, SIRC found that ODAC has not fully achieved its strategic objectives.

While SIRC noted some improvements in terms of technical infrastructure, significant issues remain with respect to business processes, governance, and performance measurement. Most problematic, SIRC found that ODAC was not able to measure the operational value of its products or the datasets.

RECOMMENDATIONS

The review was conducted at the same time as the discussions surrounding the new collection authority for datasets proposed by Bill C-59. SIRC is aware that this may put CSIS's bulk collection program on sound legal footing. Given the substantial risk that CSIS's retention and exploitation of bulk datasets exceeded its lawful mandate under the current legal framework, SIRC advised CSIS to seek direction from the Minister regarding their disposition in the interim. To date, CSIS continues to exploit the datasets.

Given the issues observed with respect to the application of current policies on datasets, SIRC is of the view that the new authorities contemplated by Bill C-59 would require rigorous governance, procedures, and training to be in place from the beginning. CSIS has indicated that it is developing a system to implement the new regime envisioned by Bill C-59, including with respect to measuring the utility of datasets. SIRC will continue to monitor this activity and the progress made by CSIS as the policy and legal framework evolves.

SIRC recommended that:

- CSIS centralize the management of all bulk datasets in order to ensure that they are assessed in a consistent and well-documented fashion.

CSIS response:

CSIS partially agreed with this recommendation.

Throughout the period of this SIRC review, CSIS was engaged in earnest efforts to fully understand the implications of Bill C-59 as it pertains to datasets and has been preparing for the new dataset regime. The spirit of this recommendation is encompassed in Bill C-59 preparations. Any immediate action that is not fully consistent with the pending legislation would not be prudent. CSIS plans to centralize all but threat related and publically available datasets within a single branch which, as per the provisions of the Bill, can only be accessible by designated employees. As for threat related datasets, SIRC is, or should be, aware that such datasets are defined in this manner because they have a clear threat nexus and therefore can be retained in CSIS's operational database. As such, datasets which meet the threat criteria will not be centralized with the datasets that will be retained under the guise of the new legislation.

It is important to note that within the past five years CSIS has undertaken a significant transformation in both its work with intelligence and its capacity to enhance it. Prior to this transformation CSIS predominantly used an unstructured reports-based system with key word search tools as its primary analytical functionality. The enhanced capacities and functions of the new integrated intelligence platform means that more complex and vast collections of threat related data can be ingested, analyzed and retained. Whether a collection of data or a single report is considered to be threat related rests on the experience, judgement, knowledge, and expertise of trained intelligence professionals. Presently, the grounds or justification for making a determination of whether something is threat related predominantly depends on human factors. Through the continued use of the new intelligence platform and the addition of performance measurement functions CSIS will soon have better metrics to assess the utility of all its collection lines. This will include a more precise understanding of how the utility of certain information diminishes over time which will help scientifically inform decisions on adequate retention periods.

CSIS has no interest in retaining any information beyond its period of utility but by the same token, it does not want to destroy information that could be critical in identifying and understanding a threat to national security. CSIS is examining the concepts of "strictly necessary" and "may assist" within a present day context which includes consideration of the en banc decision, other relevant legal decisions, as well as the wider expectations of Canadians relating to their privacy rights. Through this effort, CSIS is determined to develop new and contemporary guidance for intelligence professionals to help them make more accurate decisions about the nature of perceived threats. This guidance will also help increase CSIS's level of precision when threat assessments are made which also inform disposition and retention actions.

SIRC further recommended that:

- CSIS purge a dataset that SIRC assessed as having been unlawfully retained, both from Operational Data Analysis Centre holdings and the operational database, with the exception of records that have been used to generate threat-related reports. CSIS should also take steps to identify and purge any bulk data reported in the operational database without sufficient assessment for non-threat-related records.

CSIS response:

CSIS is in the process of assessing this recommendation.

At the point of initial collection under warrant in 2007, and again in 2016 when CSIS began to examine the legal regime applicable to datasets following a significant Federal Court decision, CSIS believed that the data in question was lawfully retained given it directly related to terrorism investigations. This is an extremely complex and important matter and requires appropriate time to conduct a full assessment. The Service is undertaking a comprehensive internal review, including the solicitation of additional legal advice from the Department of Justice. Once the review is complete, CSIS will provide the Minister of Public Safety, SIRC and the Federal Court with its assessment and response to the report. CSIS believes it would not be in the interest of national security to purge the operational data until the results of the review are known, but has restricted any access to the data in question. CSIS has also proactively advised the Federal Court of SIRC's findings on this data. It should be noted that the law surrounding the collection of personal information, and Canadians' expectations of privacy in this regard, are rapidly evolving. CSIS is committed to ensuring its data program is consistent with the *Charter* and fully respects Canadians' expectations of privacy. CSIS continues to engage with the Federal Court to ensure its warranted collection fully respects the *Charter*, Canadian law, and Canadians' reasonable expectation of privacy. In addition, the proposed changes to the *CSIS Act* in C59 will continue to ensure CSIS has a robust data program to protect Canadians in a manner that respects the *Charter* and Canadian values.

In the event that the provisions of Bill C-59 with respect to datasets become law, SIRC would see the need for further changes in their management.

Accordingly, SIRC recommended that:

- CSIS continue to prioritize the implementation of a robust process for assessing the privacy impacts and legal risk associated with its datasets, particularly with respect to Canadians.

CSIS response:

CSIS agreed with this recommendation.

The dataset framework introduced in Bill C-59 will effectively address legal risks and potential privacy impacts. New processes, systems, and policies are being developed to ensure CSIS is prepared to implement the bill.

SIRC further recommended that:

- CSIS develop a system for assessing the utility of individual datasets, and that decisions regarding the continued retention of datasets should be informed by those assessments.

CSIS response:

CSIS agreed with the overall recommendation, however, it disagreed with SIRC's conclusion regarding the utility of data analytics and questioned the validity of SIRC's assessment methodology. Data analytics is an effective means for generating leads, providing or corroborating intelligence, and advancing investigations. CSIS is developing a system for assessing the utility of individual datasets and for integrating these assessments into decisions regarding the retention of a dataset. The record keeping requirements under Bill C-59, along with enhanced storage and analytic systems, will allow for additional validation of retained datasets based on operational utility.

SIRC further recommended that:

- CSIS implement as soon as practicable a data control system in its operational database that ensures that each piece of reported data from bulk datasets is appropriately tracked and managed.

CSIS response:

CSIS agreed with this recommendation.

Within CSIS' data holdings, governance systems have already been introduced to track the provenance and life cycle of data elements. Bill C-59 requirements will further enhance existing access controls, including limiting access to designated employees.

SIRC further recommended that:

- CSIS develop a strategic approach to data collection and analysis across the organization, including with respect to data governance, performance measurement, and the integration of data analysis with investigations.

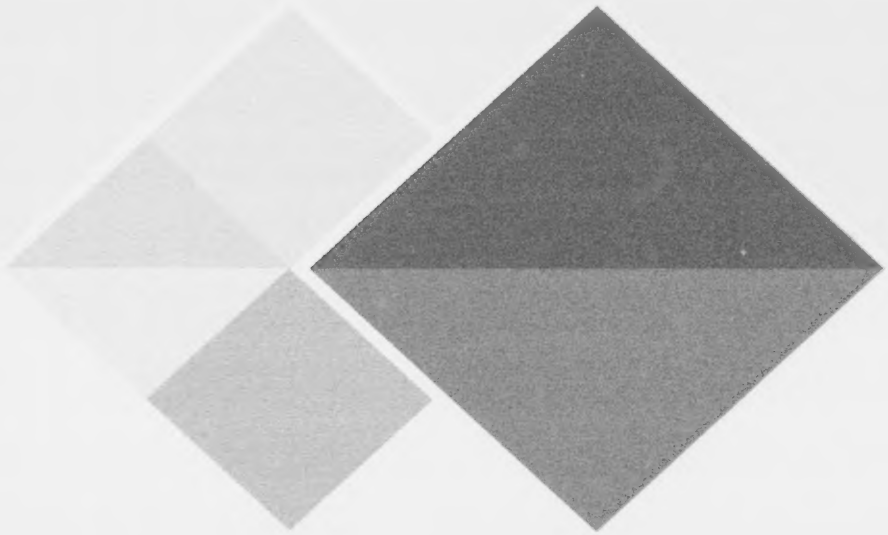
CSIS response:

CSIS agreed with this recommendation.

CSIS achieved its strategic objectives as defined by the 2005 Data Exploitation Task Force. CSIS is striving towards an enhanced strategic approach to data collection and analysis as per Bill C-59.

The en banc decision of October 2016 provided definitive interpretation of CSIS obligations with respect to retention and analysis, leading to significant efforts to realign collection, retention, and analysis to ensure compliance.

4 COMPLAINT INVESTIGATIONS



Under the CSIS Act, *one of SIRC's core functions is to investigate complaints in the following instances:*

- with respect to **any act or thing** done by CSIS (section 41 of the *CSIS Act*); and
- with respect to the denial or revocation of a security clearance necessary to obtain or keep federal government employment or contracts (section 42 of the *CSIS Act*).

SIRC also has the mandate to conduct investigations into reports made to it pursuant to section 19 of the *Citizenship Act*, and into matters referred pursuant to section 45 of the *Canadian Human Rights Act*.

THE COMPLAINT PROCESS AT SIRC

Complaint cases at SIRC may begin as inquiries to the Committee either in writing or by phone. Once received, staff will advise the prospective complainant about the requirements of the *CSIS Act* and SIRC's Rules of Procedure for initiating a formal complaint.

Once the formal complaint is received, a preliminary review is conducted, which can include information that may be in the possession of CSIS, with the exception of Cabinet confidences. If the complaint does not meet certain statutory requirements, SIRC is obligated to decline on the basis of jurisdiction (see "How SIRC Determines Jurisdiction of a Complaint" on page 35), and the complaint is not investigated further.

If jurisdiction is established, the complaint will be investigated through a quasi-judicial hearing, presided over by a Committee member. The member is assisted by members of SIRC's staff and legal team, who provide legal advice on procedural and substantive matters.

A pre-hearing conference is conducted with all parties to establish and agree on preliminary procedural matters, such as the allegations to be investigated, the format of the hearing, the identity and number of witnesses to be called, the disclosure of documents in advance of the hearing, and the date and location of the hearing.

The investigation and resolution of a complaint will vary in length depending on a number of factors, such as the complexity of the file, the quantity of documents to be examined, the number of hearing days required, the availability of the participants, and the various procedural matters raised by the parties.

SIRC investigations are to be conducted "in private," as per the *CSIS Act*. All parties have the right to be represented by counsel, to present evidence, to make representations, and to be heard in person at a hearing, but no one is entitled as of right to be present during, to have access to, or to comment on, representations made to SIRC by any other person.

A party may request an *ex parte* hearing (in the absence of the other parties) to present evidence that, for reasons of national security or other reasons considered valid by SIRC, cannot be disclosed to the other party or their counsel. During such hearings, SIRC's legal team will cross-examine the witnesses to ensure that the evidence is appropriately tested and reliable. This provides the presiding Committee member with the most complete and accurate factual information relating to the complaint.

Once the *ex parte* portion of the hearing is completed, SIRC will determine whether the substance of the evidence can be disclosed to the excluded parties. If so, SIRC will prepare a summary of the evidence and provide it to the excluded parties once it has been vetted for national security concerns.

On completion of an investigation, SIRC issues a final report containing its findings and recommendations, if any. A copy of the report is then provided to the Director of CSIS, the Minister of Public Safety and Emergency Preparedness and, in the case of a security clearance denial, to the deputy head concerned. A declassified version of the report is also provided to the complainant.

ALLEGATIONS OF RELIGIOUS PROFILING AND CONSPIRACY: COMPLAINT PURSUANT TO SECTION 41 OF THE *CSIS ACT*

SIRC investigated a complaint under section 41 of the *CSIS Act* that addressed the following issues: (1) whether CSIS officers, while dealing with the complainant, asked questions and made requests that amounted to religious profiling; and (2) whether CSIS was involved in a conspiracy with another government department against the complainant and his organization.

HOW SIRC DETERMINES JURISDICTION OF A COMPLAINT...

...under section 41 of the CSIS Act

SIRC shall investigate complaints made by "any person" with respect to "any act or thing done by the Service." Before SIRC investigates, two conditions must be met:

1. *The complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and*
2. *SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious, or made in bad faith.*

SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the CSIS Act *or the* Federal Public Sector Labour Relations Act.

...under section 42 of the CSIS Act

SIRC shall investigate complaints from:

1. *any person refused federal employment because of the denial of a security clearance;*
2. *any federal employee who is dismissed, demoted, transferred, or denied a transfer or promotion for the same reason; or*
3. *anyone refused a contract to supply goods or services to the government for the same reason.*

These types of complaints must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

SIRC found that the allegations with regards to religious profiling were unsupported, and that questions and requests posed to the complainant by CSIS agents were conducted within legal and policy guidelines. In relation to the conspiracy allegation, the complainant provided evidence that he and his organization had been through some difficulties and he alleged that CSIS had conspired to organize these difficulties. SIRC found that CSIS was not involved in the events in question. SIRC concluded that CSIS did not conspire against the complainant and his organization, and that there was no evidence of actions that contravene law or policy.

In summary, SIRC found that the conduct of CSIS investigations remained focused on threats to the security of Canada. For these reasons, the complaint was dismissed.

ALLEGATIONS OF DELAY AND RACIAL PREJUDICE IN A VISA APPLICATION: COMPLAINT PURSUANT TO SECTION 41 OF THE *CSIS ACT*

SIRC investigated a complaint under section 41 of the *CSIS Act* that addressed the following issues: (1) the delay in processing the complainant's visa application was too long; (2) the visa application was denied due to racial profiling based on the complainant's nationality; and (3) the visa application was denied based on unfounded assumptions.

The complainant attributed the delays in the processing of his initial and subsequent visa application to the actions of CSIS. The total time taken by CSIS after receiving the request for security advice from the Canada Border Services Agency (CBSA) was approximately six months. SIRC concluded that CSIS provided its assessment to the CBSA within a reasonable delay. Based on all of the evidence, SIRC did not attribute any subsequent delays leading up to the decision made by Immigration, Refugees, and Citizenship Canada (IRCC) on the complainant's second visa application to any act or thing done by CSIS, as no further information was disseminated to CSIS after it provided its advice to the CBSA in response to the first visa application.

Concerns arose in the course of the investigation with regard to the complainant's perception that CSIS contributed to the delay from the time CSIS provided its assessment to CBSA, and IRCC's decision that he was inadmissible to Canada. SIRC found that although the reason for the delays in processing the complainant's visa applications were not clear, insofar as the actions taken by CBSA and IRCC following CSIS's assessment of the complainant's first visa application, it appears that there could be room to continue generally improving processes among the three partners. Therefore, the Committee requested further documentary evidence from CSIS and, specifically, copies of memoranda of understanding (MOUs).

With respect to the other allegations, SIRC found that CSIS's assessment was not based on racial prejudice or on unfounded assumptions, as alleged by the complainant.

For these reasons, SIRC concluded that all three of the complainant's allegations were unsupported and the complaint was dismissed.

SIRC recommended that:

- CSIS continue its efforts in collaborating with CBSA and IRCC for the creation of annexes to the MOUs.

CSIS response:

CSIS agreed with this recommendation.

CSIS will continue to work with both CBSA and IRCC to create annexes to the MOUs.

ALLEGATIONS THAT CSIS COLLECTED INFORMATION ABOUT CANADIAN CITIZENS AND GROUPS ENGAGED IN PEACEFUL AND LAWFUL ACTIVITIES: COMPLAINT PURSUANT TO SECTION 41 OF THE *CSIS ACT*

SIRC investigated a complaint pursuant to section 41 of the *CSIS Act* in which the complainant alleges that CSIS has investigated groups or individuals for their engagement in lawful advocacy, protest, or dissent activities. In addition, the complainant alleged that CSIS shared intelligence information with other government departments and the private sector. SIRC found no evidence that CSIS collected information or investigated any peaceful advocacy or dissent and that all collection of information was in accordance with section 12 of the *CSIS Act*.

With regard to information sharing, evidence showed that CSIS did not disseminate information among government bodies and private sector organizations. Any information released was as a result of ATIP requests. SIRC found that CSIS fulfilled its mandate of "reporting and advising," and had the obligation to provide reports and advice to the Government of Canada in accordance with its enabling legislation.

For these reasons, the Committee found that the complainant's allegations were not supported by the evidence and, therefore, the complaint was dismissed.

SIRC recommended that:

- CSIS prioritize inclusive public discussions with the groups involved in the present complaint, where possible, having regard to the classified nature of certain topics.

CSIS response:

CSIS partially agreed with this recommendation; this will be considered in the context of a broader stakeholder engagement strategy.

CSIS routinely communicates with Canadians and stakeholders to explain our mandate. This is done not only to inform but to seek community support. It is believed that a well-informed community is more likely to be part of the National Security solution.

DENIAL OF SECURITY CLEARANCE: COMPLAINT PURSUANT TO SECTION 42 OF THE *CSIS ACT*

SIRC investigated a complaint pursuant to section 42 of the *CSIS Act* concerning the denial of the complainant's secret security clearance by a Department. SIRC found that

there were reasonable grounds for the Deputy Head to have denied the complainant's secret security clearance based on the information that was available as a result of the security screening process.

The complainant had suspected that CSIS discriminated against the complainant due to ethnic heritage, preconceived notions, education, and international experience. After considering the evidence presented, SIRC found no indication that there was any discrimination as part of the security screening process.

The complainant also took issue with the length of the period of assessment of the denial of their clearance. SIRC found that the length of time for the assessment of the clearance was not unreasonable in the circumstances of this case.

SIRC ultimately recommended that the decision to deny the security clearance be upheld and dismissed the complaint.

Nevertheless, SIRC recommended that:

- CSIS, as the centre for the assessment of security clearances, should, through means it deems appropriate, continue to stress to its client departments and agencies the importance of compliance with the clearance regime.

CSIS response:

CSIS agreed with the recommendation.

Under the Policy on Government Security (PGS), CSIS has a role as a Lead Security Agency to do outreach related to security clearance screening, and we do so through engagement with the Departmental Security Officer (DSO) community which functions as a center of excellence. The risk assessed by each DSO and mitigation of the risk of granting the clearance falls to each DSO and is within the power of each department. The role of evaluating compliance with the PGS or the Standard for Security Screening falls to the individual Department and to TBS.

SIRC further recommended that:

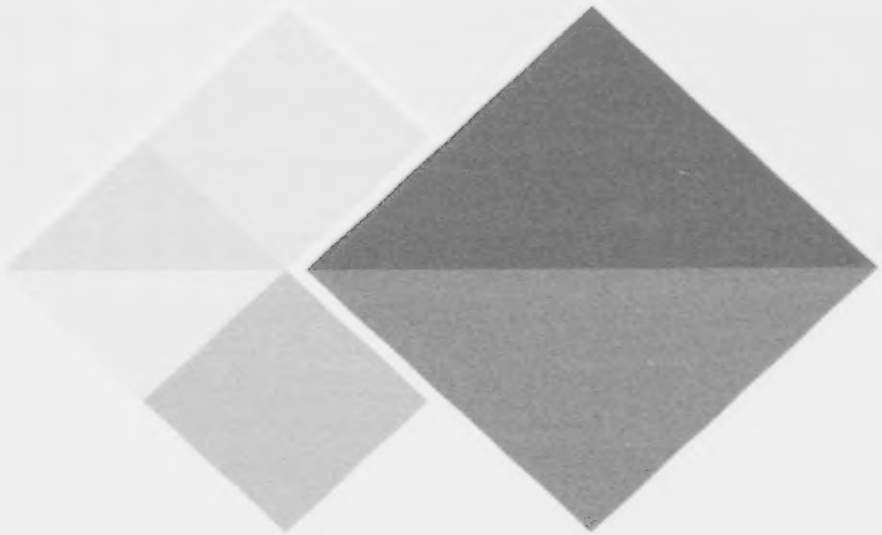
- CSIS arrange to have additional resources available for clearances in times of foreseeable increases in clearance requests in order to reduce the possibility of delays in staffing.

CSIS response:

CSIS agreed with the recommendation.

CSIS has cross trained its security screening resources to be able to more effectively respond to security screening surges. CSIS also works with client departments to receive advance warning on surges in all screening areas and to establish manageable timelines.

5 RECOMMENDATIONS



Review	SIRC recommended that...	CSIS response
Case Studies Regarding CSIS Information Sharing with Foreign Entities	▶ CSIS prioritize the development of guidelines on assessing and documenting the risk of mistreatment, as well as the risks of assurances and caveats not being respected. Such assessments should take into account the most recent and relevant information, including operational reporting.	CSIS agreed with this recommendation. In addition to robust existing guidelines on assessing and documenting the risk of mistreatment, CSIS is adopting a new model for restricting exchanges with foreign agencies. This new approach has three clear objectives: (a) ensuring that CSIS' engagement with a foreign partner does not pose a substantial risk of mistreatment; (b) only allow sharing of information which is not deemed to present a potential risk of mistreatment; and (c) ensuring full compliance with the Ministerial Directive.

Review	SIRC recommended that...	CSIS response
	▸ When there is a substantial risk of mistreatment in sharing or requesting information that needs to be mitigated, the decision to share should be referred to the Director through the Information Sharing Evaluation Committee, rather than an operational manager.	CSIS agreed with this recommendation. Ministerial Direction is enshrined within CSIS directives on information sharing when there is a risk of mistreatment. Moreover, CSIS has adopted a new model for restricting exchanges with foreign agencies in which proposed exchanges of information deemed to be high risk must automatically be referred to the Information Sharing Evaluation Committee (ISEC) and others will be prohibited outright.
CSIS's Approach to Mental Health	▸ CSIS increase the resources available to keep up with the demands for services that assist CSIS to manage mental health issues that arise in CSIS investigations.	CSIS partially agreed with this recommendation. CSIS has been working to address vacancies and has also explored other strategies to increase these capabilities. CSIS will consider these requirements in any future resource allocation exercises, while also taking into account competing requirements in other priority areas.
	▸ CSIS create a specific reference tool to be relied upon to identify general mental health issues.	CSIS agreed with this recommendation. CSIS sees value in the creation of this tool as it will assist CSIS officers in identifying general mental health issues in a proactive fashion.
CSIS's Right-Wing Extremism Investigation	▸ CSIS determine the extent to which other regions' investigation of right-wing extremism could benefit from the experience of CSIS's law enforcement collaborative model in place in the Québec Region.	CSIS agreed with this recommendation. Mechanisms are in place across all regions to ensure effective collaboration exists between CSIS and domestic law enforcement bodies.
CSIS's Use of the Internet in Support of Operations	▸ CSIS ask Justice Canada to conduct a comprehensive legal review of this program.	CSIS agreed with this recommendation. CSIS will request that Justice Canada undertake a legal review of key aspects of the use of internet in support of operations. CSIS will continue to adhere to policies and directives on the administration of this program and will seek out legal advice when and where appropriate.
	▸ CSIS ensure that those individuals currently engaged in these operations be given training as soon as possible.	CSIS agreed with this recommendation. It is standard CSIS practice to ensure designated employees receive the appropriate training.

Review	SIRC recommended that...	CSIS response
Foreign Stations	▸ CSIS institute a quality assurance mechanism to ensure all required caveats are included prior to sharing information with its partners.	CSIS agreed with this recommendation. CSIS is preparing updates to caveat policies and procedures that will further improve quality assurance. Furthermore, CSIS is developing training and technological support related to the use of caveats.
CSIS Operations in Dangerous Environments	CSIS develop a comprehensive strategic framework for operating within dangerous environments. The strategic framework should address, among other considerations, the following: ▸ creating a more sophisticated rationale for designating dangerous environments, and considering the associated implications of such a designation; ▸ specifying requirements for employee training pre-deployment; ▸ updating policies and standard operating procedures; ▸ clarifying stakeholder roles and responsibilities; ▸ clarifying expectations for and current feasibility of foreign operational support team(s) who provide a number of crucial services for employees deployed in dangerous environments; and ▸ developing a communications plan between management and employees specifically geared toward high-risk deployments.	CSIS agreed with this recommendation and will incorporate and update existing guidelines, policies, and procedures into this framework.

SECTION 54 REPORT:
CSIS'S RESPONSE TO THE FEDERAL COURT DECISION OF OCTOBER 2016

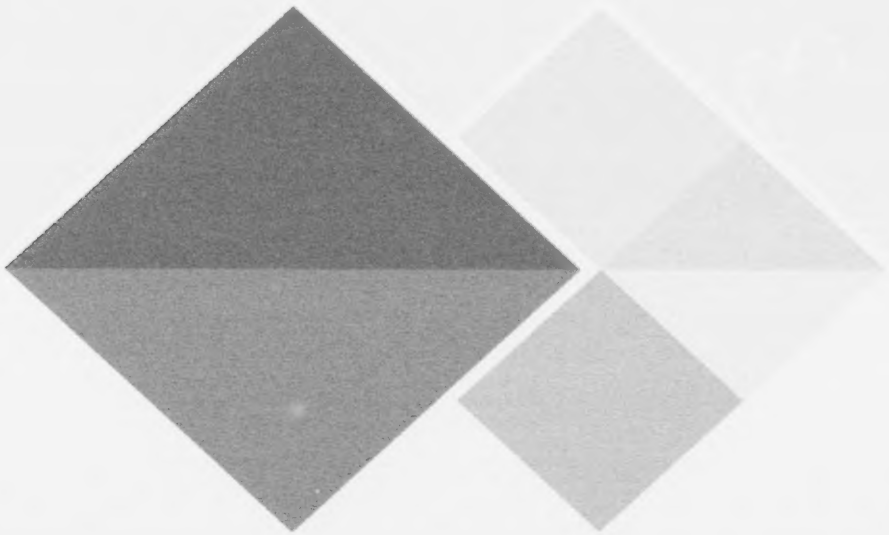
SIRC recommended that...	CSIS response
CSIS centralize the management of all bulk datasets in order to ensure that they are assessed in a consistent and well-documented fashion.	CSIS partially agreed with this recommendation. Throughout the period of this SIRC review, CSIS was engaged in earnest efforts to fully understand the implications of Bill C-59 as it pertains to datasets and has been preparing for the new dataset regime. The spirit of this recommendation is encompassed in Bill C-59 preparations. Any immediate action that is not fully consistent with the pending legislation would not be prudent. CSIS plans to centralize all but threat related and publically available datasets within a single branch which, as per the provisions of the Bill, can only be accessible by designated employees. As for threat related datasets, SIRC is, or should be, aware that such datasets are defined in this manner because they have a clear threat nexus and therefore can be retained in CSIS's operational database. As such, datasets which meet the threat criteria will not be centralized with the datasets that will be retained under the guise of the new legislation. It is important to note that within the past five years CSIS has undertaken a significant transformation in both its work with intelligence and its capacity to enhance it. Prior to this transformation CSIS predominantly used an unstructured reports-based system with key word search tools as its primary analytical functionality. The enhanced capacities and functions of the new integrated intelligence platform means that more complex and vast collections of threat related data can be ingested, analyzed and retained. Whether a collection of data or a single report is considered to be threat related rests on the experience, judgement, knowledge, and expertise of trained intelligence professionals. Presently, the grounds or justification for making a determination of whether something is threat related predominantly depends on human factors. Through the continued use of the new intelligence platform and the addition of performance measurement functions CSIS will soon have better metrics to assess the utility of all its collection lines. This will include a more precise understanding of how the utility of certain information diminishes over time which will help scientifically inform decisions on adequate retention periods. CSIS has no interest in retaining any information beyond its period of utility but by the same token, it does not want to destroy information that could be critical in identifying and understanding a threat to national security. CSIS is examining the concepts of "strictly necessary" and "may assist" within a present day context which includes consideration of the en banc decision, other relevant legal decisions, as well as the wider expectations of Canadians relating to their privacy rights. Through this effort, CSIS is determined to develop new and contemporary guidance for intelligence professionals to help them make more accurate decisions about the nature of perceived threats. This guidance will also help increase CSIS's level of precision when threat assessments are made which also inform disposition and retention actions.

SIRC recommended that...	CSIS response
▸ CSIS purge a dataset that SIRC assessed as having been unlawfully retained, both from Operational Data Analysis Centre holdings and the operational database, with the exception of records that have been used to generate threat-related reports. CSIS should also take steps to identify and purge any bulk data reported in the operational database without sufficient assessment for non-threat-related records.	CSIS is in the process of assessing this recommendation. At the point of initial collection under warrant in 2007, and again in 2016 when CSIS began to examine the legal regime applicable to datasets following a significant Federal Court decision, CSIS believed that the data in question was lawfully retained given it directly related to terrorism investigations. This is an extremely complex and important matter and requires appropriate time to conduct a full assessment. The Service is undertaking a comprehensive internal review, including the solicitation of additional legal advice from the Department of Justice. Once the review is complete, CSIS will provide the Minister of Public Safety, SIRC and the Federal Court with its assessment and response to the report. CSIS believes it would not be in the interest of national security to purge the operational data until the results of the review are known, but has restricted any access to the data in question. CSIS has also proactively advised the Federal Court of SIRC's findings on this data. It should be noted that the law surrounding the collection of personal information, and Canadians' expectations of privacy in this regard, are rapidly evolving. CSIS is committed to ensuring its data program is consistent with the *Charter* and fully respects Canadians' expectations of privacy. CSIS continues to engage with the Federal Court to ensure its warranted collection fully respects the *Charter*, Canadian law, and Canadians' reasonable expectation of privacy. In addition, the proposed changes to the *CSIS Act* in C59 will continue to ensure CSIS has a robust data program to protect Canadians in a manner that respects the *Charter* and Canadian values.
In the event that the dataset provisions of Bill C-59 become law, SIRC further recommended that:	
▸ CSIS continue to prioritize the implementation of a robust process for assessing the privacy impacts and legal risk associated with its datasets, particularly with respect to Canadians.	CSIS agreed with this recommendation. The dataset framework introduced in Bill C-59 will effectively address legal risks and potential privacy impacts. New processes, systems, and policies are being developed to ensure CSIS is prepared to implement the bill.

SIRC recommended that...	CSIS response
▸ CSIS develop a system for assessing the utility of individual datasets, and that decisions regarding the continued retention of datasets should be informed by those assessments.	CSIS agreed with the overall recommendation, however, it disagreed with SIRC's conclusion regarding the utility of data analytics and questioned the validity of SIRC's assessment methodology. Data analytics is an effective means for generating leads, providing or corroborating intelligence, and advancing investigations. CSIS is developing a system for assessing the utility of individual datasets and for integrating these assessments into decisions regarding the retention of a dataset. The record keeping requirements under Bill C-59, along with enhanced storage and analytic systems, will allow for additional validation of retained datasets based on operational utility.
▸ CSIS implement as soon as practicable a data control system in its operational database that ensures that each piece of reported data from bulk datasets is appropriately tracked and managed.	CSIS agreed with this recommendation. Within CSIS' data holdings, governance systems have already been introduced to track the provenance and life cycle of data elements. Bill C-59 requirements will further enhance existing access controls, including limiting access to designated employees.
▸ CSIS develop a strategic approach to data collection and analysis across the organization, including with respect to data governance, performance measurement, and the integration of data analysis with investigations.	CSIS agreed with this recommendation. CSIS achieved its strategic objectives as defined by the 2005 Data Exploitation Task Force. CSIS is striving towards an enhanced strategic approach to data collection and analysis as per Bill C-59. The en banc decision of October 2016 provided definitive interpretation of CSIS obligations with respect to retention and analysis, leading to significant efforts to realign collection, retention, and analysis to ensure compliance.

Complaint	SIRC recommended that...	CSIS response
Allegations of Delay and Racial Prejudice in a Visa Application: Complaint Pursuant to Section 41 of the *CSIS Act*	▸ CSIS continue its efforts in collaborating with CBSA and IRCC for the creation of annexes to the MOUs.	CSIS agreed with this recommendation. CSIS will continue to work with both CBSA and IRCC to create annexes to the MOUs.
Allegations That CSIS Collected Information about Canadian Citizens and Groups Engaged in Peaceful and Lawful Activities (Section 41 of the *CSIS Act*)	▸ CSIS prioritize inclusive public discussions with the groups involved in the present complaint, where possible, having regard to the classified nature of certain topics.	CSIS partially agreed with this recommendation; this will be considered in the context of a broader stakeholder engagement strategy. CSIS routinely communicates with Canadians and stakeholders to explain our mandate. This is done not only to inform but to seek community support. It is believed that a well-informed community is more likely to be part of the National Security solution.
Denial of Security Clearance: Complaint Pursuant to Section 42 of the *CSIS Act*	▸ CSIS, as the centre for the assessment of security clearances, should, through means it deems appropriate, continue to stress to its client departments and agencies the importance of compliance with the clearance regime.	CSIS agreed with the recommendation. Under the Policy on Government Security (PGS), CSIS has a role as a Lead Security Agency to do outreach related to security clearance screening, and we do so through engagement with the Departmental Security Officer (DSO) community which functions as a center of excellence. The risk assessed by each DSO and mitigation of the risk of granting the clearance falls to each DSO and is within the power of each department. The role of evaluating compliance with the PGS or the Standard for Security Screening falls to the individual Department and to TBS.
	▸ CSIS arrange to have additional resources available for clearances in times of foreseeable increases in clearance requests in order to reduce the possibility of delays in staffing.	CSIS agreed with the recommendation. CSIS has cross trained its security screening resources to be able to more effectively respond to security screening surges. CSIS also works with client departments to receive advance warning on surges in all screening areas and to establish manageable timelines.

6 CORPORATE OPERATIONS



BUDGET

TABLE 1 EXPENDITURES

Program	2016–2017 Expenditures	2017–2018 Planned Spending	2017–2018 Actual Spending	2018–2019 Planned Spending
Reviews	1,670,700	2,344,000	2,343,984	2,327,933
Legal Services	980,500	1,429,600	1,429,665	1,409,230
Subtotal	2,651,200	3,773,600	3,773,649	3,737,163
Internal Services*	1,823,500	1,247,700*	3,247,697	1,396,677
TOTAL	4,474,700	5,021,300	7,021,346	5,133,840

*Internal Services are those groups of related activities and resources that the federal government considers to be services in support of Programs and/or required to meet corporate obligations of an organization. Internal Services refers to the activities and resources of the 10 distinct service categories that support Program delivery in the organization, regardless of the Internal Services delivery model in a department. The 10 service categories are: Management and Oversight Services; Communications Services; Legal Services; Human Resources Management Services; Financial Management Services; Information Management Services; Information Technology Services; Real Property Services; Materiel Services; and Acquisition Services.

OUTREACH

SIRC once again participated in a number of outreach activities, including presentations at universities and conferences, and appearances before parliamentary committees, including the following highlights:

APRIL 2017

SIRC's research team gave a presentation on SIRC's structure and mandate to an undergraduate class on intelligence and international relations at the University of Ottawa.

SEPTEMBER 2017

SIRC's Executive Director was in regular contact with the University of Calgary's law school and provided material that was used in the teaching of the law school's National Security Law Laboratory program.

OCTOBER 2017

The Committee Chairman co-hosted, along with Commissioner Plouffe of the Office of the Communications Security Establishment Commissioner, the first meeting of the Five Eyes Intelligence Oversight and Review Council (FIORC), the objective of which is to foster closer linkages within the Five Eyes review and oversight community. Representatives of review bodies from all Five Eyes countries participated.

NOVEMBER 2017

SIRC hosted a delegation from the Italian Parliamentary Committee for the Security of the Republic.

DECEMBER 2017

SIRC's legal and research team gave a presentation on SIRC's structure and mandate to a national security law class at the University of Ottawa.

JANUARY 2018

SIRC participated from January to April 2018 in the Capstone Project of the University of Toronto's Munk School of Global Affairs. This is part of the curriculum of the Munk School's master's program involving a team of three to four students doing research on a "real world" problem relevant to public administration. This year, SIRC was identified as one of a number of government partners.

FEBRUARY 2018

On February 8, 2018, the Chairman and acting Executive Director of SIRC appeared before the Standing Committee on Public Safety and National Security (SECU) on the subject of Bill C-59.

MARCH 2018

SIRC's legal and research team participated in a half-day roundtable discussion on national security and accountability at a class offered by the Université de Sherbrooke along with other members of the intelligence accountability system.

SIRC CHAIRMAN'S APPEARANCE BEFORE THE STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY

On February 8, 2018 during his appearance before the Standing Committee on Public Safety and National Security (SECU) on the subject of Bill C-59, SIRC's Chairman provided SECU with a list of amendments to improve and clarify certain aspects of the bill. These are available on SIRC's website: www.sirc-csars.gc.ca/opbapb/index-eng.html.

7 ANNEX

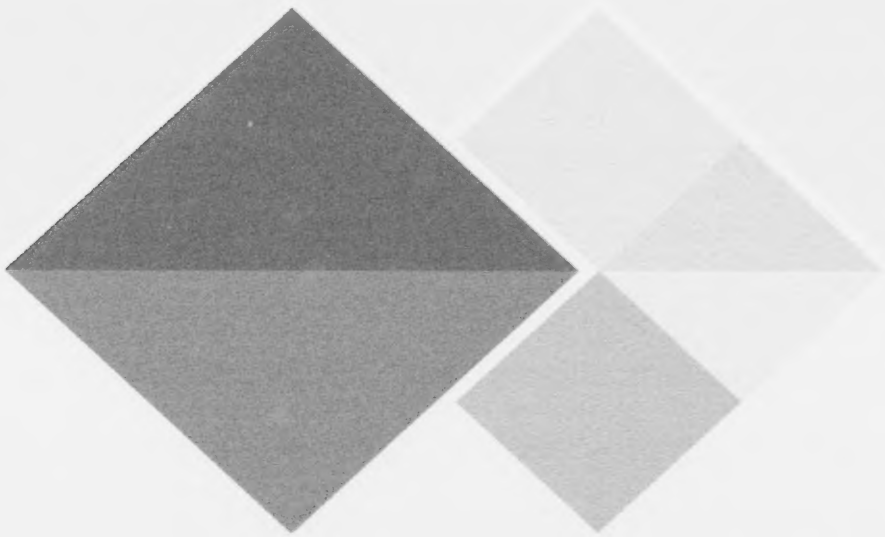


TABLE 2 TARGETING

CSIS may investigate a person or group engaged in activities suspected of posing a threat to the security of Canada. Section 2 of the *CSIS Act* defines these activities as being in support of espionage, sabotage, foreign-influenced activity, or terrorism. This table indicates the number of targets (rounded to the nearest 10) investigated by CSIS in the past three fiscal years.

	2015–2016	2016–2017	2017–2018
Targets	550	560	500

TABLE 3 WARRANTS

The warrant statistics found here represent the total number of warrant applications granted by the Federal Court, independent of the actual number of warrants granted in each application or the number of individuals who were the subject of warrants.

	2015–2016	2016–2017	2017–2018
New	14	11	13
Replacement or Supplemental	22	18	23
Total	36	29	36

TABLE 4 COMPLAINTS

Program	2017–2018
Intakes	63
Complaints Carried Over from Previous Fiscal Year	16
New Complaints*	15
Total	31
Files Closed	18
Files Carried Forward	13

*Met statutory requirements.